

**Notice of Allowability**

Application No.

10/086,516

Examiner

Eleni A. Shiferaw

Applicant(s)

NGUYEN ET AL.

Art Unit

2136

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 10/10/2006.
2. ☒ The allowed claim(s) is/are 1-13, 24, 26, 28, and 30-53.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some\* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.


Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),  
Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit  
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),  
Paper No./Mail Date 10/18/06
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

  
10/20/06

### DETAILED ACTION

1. Allowable subject matter was provided to the applicant on the final action mailed on 08/07/2006. Applicant complied with the examiner's objections to move dependent claims to the base claims. The appellant's claims raised 101 issues that were resolved by the agreement on the telephone interview with Ronald M. Pomeranke on October 18, 2006. Based on the interview, Examiner's amendment has been made for independent claim 24.
2. Claims 14-23, 25, 27, and 29 are canceled.

### EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Ronald M. Pomeranke on October 18, 2006.

3. Claim 24 is amended as follows.
24. (Currently Amended) A computer-readable storage medium storing ~~carrying~~ one or more sequences of instructions for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transport protocol, which instructions, when executed by one or more processor, cause the one or more

processor to carry out the steps of:

selecting a subset of data for encryption from a set of data to be communicated between the client and the server in a particular payload of the unencrypted transfer protocol;

determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads, wherein the secret integer associated with the particular payload is unique relative to secret integers associated with other payloads of the plurality of payloads, wherein determining the secret integer comprising:

determining a shared secret key based on a first integer and a first public key associated with a receiving device of the client and the server; and

selecting the secret integer based on the shared secret key;

encrypting the subset of data using at least the secret integer to generate encrypted data that is practically unintelligible to a device other than the client and server; and

sending, from a sending device of the client and the server to the receiving device, in the particular payload, the encrypted data and information to determine, only at the client and the server, the secret integer for decrypting the encrypted data.

***Allowable Subject Matter***

3. The following is a statement of reasons for the indication of allowable:

Claims 1-13, 24, 26, 28, and 30-53 are allowed.

The prior art made of record neither alone nor in combination teach a method/medium/apparatus for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transfer

protocol comprising selecting a subset of data for encryption from a set of data to be communicated, determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads, wherein the secret integer associated with the particular payload is unique relative to secret integers associated with other payloads of the plurality of payloads, wherein the determining steps comprises determining a shared secret key based on a first integer and a first public key associated with a receiving device and selecting the secret integer based on the shared secret key, and encrypting the subset of data using the secret integer and sending the encrypted data, clue information, and the secret integer for decrypting encrypted data in the particular payload.

Claims 2-13, 30-41, and 42-53 are allowed because of dependency.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

### ***Conclusion***

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

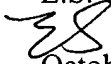
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for

Art Unit: 2136


the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

E.S.

  
October 18, 2006

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

  
10/20/06